Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

Ufficio federale di giustizia UFG
Ambito direzionale Servizi centrali
Settore Informatica giuridica

Requisiti per le piattaforme per la trasmissione sicura in ambito procedurale (Catalogo dei requisiti per le piattaforme di trasmissione)

del 16 settembre 2014 (Versione 2.0)

Allegato all'ordinanza del DFGP del 16 settembre 2014 sul riconoscimento di piattaforme per la trasmissione sicura in ambito procedurale (Ordinanza sul riconoscimento di piattaforme di trasmissione; RS 272.11)

Indice

1 Scopo e contenuti

[1] Il presente catalogo specifica i requisiti per le piattaforme di trasmissione secondo l'articolo 2 dell'ordinanza sul riconoscimento di piattaforme di trasmissione.

[2] Le piattaforme di trasmissione riconosciute possono essere impiegate anche per la comunicazione per via elettronica nell'ambito di procedimenti amministrativi. Le decisioni di riconoscimento del Dipartimento federale di giustizia e polizia (DFGP) sono dunque anche applicabili all'ordinanza del 18 giugno 2010 sulla comunicazione per via elettronica nell'ambito di procedimenti amministrativi (OCE-PA; RS 172.021.2).

2 Elementi principali dei messaggi elettronici

Un messaggio elettronico è composto da un'intestazione (header) e un corpo (body), eventualmente completato da uno o più allegati. Il corpo e gli allegati sono denominati componenti.

3 Coinvolgimento di terzi

Il titolare del riconoscimento (fornitore di prestazioni) può delegare parzialmente o totalmente a terzi l'esercizio tecnico della piattaforma, continuando ad assumersene la responsabilità tecnica, amministrativa, giuridica e gestionale.

4 Requisiti relativi alla sicurezza delle informazioni

4.1 Requisiti fondamentali per imprese private

[1] Se il fornitore di prestazioni è un'impresa privata, la sicurezza delle informazioni deve essere garantita mediante l'installazione, l'implementazione, l'esercizio, la sorveglianza, il controllo, la manutenzione e il miglioramento di un sistema di gestione della sicurezza delle informazioni (Information Security Management System, ISMS) che soddisfa i criteri della norma SN EN ISO/IEC 27001 (2013 Information technology – Security techniques – Information security management systems – Requirements[1]).

[2] L'efficacia e l'adeguatezza dell'ISMS devono essere comprovate mediante un certificato conforme alla norma SN EN ISO/IEC 27001, 2013, rilasciato da un servizio di certificazione accreditato dal Servizio di accreditamento svizzero (SAS). Le prestazioni offerte dalla piattaforma di trasmissione devono essere comprese nel campo d'applicazione dell'ISMS certificato. Fino alla scadenza del termine di transizione adottato dalla SAS è riconosciuto anche un

[1] La norma può essere consultata e richiesta presso l'Associazione svizzera di normazione (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

certificato conforme alla SN EN ISO/IEC 27001, 2005 (Information technology – Security techniques – Information security management systems – Requirements[2]).

[3] In caso di pubblicazione di una nuova versione della norma SN EN ISO/IEC 27001, deve essere presentato al più tardi alla scadenza del termine di transizione un certificato valido dell'ISMS secondo questa nuova versione. Le prestazioni offerte dalla piattaforma di trasmissione devono però continuare a essere comprese nel campo d'applicazione dell'ISMS certificato.

4.2 Requisiti fondamentali per autorità

[1] Se il fornitore di prestazioni è un'autorità rimane indispensabile un ISMS conforme alla SN EN ISO/IEC 27001, 2013, ma in casi eccezionali motivati è possibile rinunciare a un certificato formale rilasciato da un servizio di certificazione riconosciuto. In questo caso l'efficacia e l'adeguatezza dell'ISMS devono essere comprovati presentando un rapporto sui risultati dell'audit formale interno effettuato sull'ISMS conformemente alla clausola 9.2 della SN EN ISO/IEC 27001, 2013. Il rapporto di audit non può comprendere alcun elemento che potrebbe opporsi a una certificazione. Fino alla scadenza del termine di transizione adottato dalla SAS, il riconoscimento è possibile anche sulla base di un rapporto sui risultati dell'audit formale interno effettuato sull'ISMS conformemente alla clausola 6 della SN EN ISO/IEC 27001, 2005.

[2] I principi e l'esecuzione degli audit, nonché le competenze e l'esperienza degli auditori si fondano sulle norme SN EN ISO/IEC 19011, 2011 (Guidelines for auditing management systems[3]) e SN EN ISO/IEC 27007, 2011 (Information technology – Security techniques – Guidelines for information security management systems auditing[4]). L'audit deve essere ripetuto almeno ogni anno e i relativi rapporti devono essere presentati all'UFG.

[3] In caso di pubblicazione di una nuova versione della norma SN EN ISO/IEC 27001, la conformità dell'ISMS deve essere dimostrata mediante il rapporto di audit interno entro la scadenza del termine di transizione. Le prestazioni offerte dalla piattaforma di trasmissione devono però continuare a essere comprese nel campo d'applicazione dell'ISMS certificato.

4.3 Requisiti supplementari per imprese private e autorità

I requisiti descritti ai punti 4.3.1 - 4.3.3 devono essere considerati nell'ambito della gestione del rischio ai sensi della SN EN ISO/IEC 27005, 2011.

4.3.1 Gestione dell'esercizio e della comunicazione

[1] La gestione dell'esercizio della piattaforma di trasmissione e delle comunicazioni per le quali è utilizzata deve orientarsi allo stato della tecnica, essere oggetto di una descrizione completa e dettagliata ed essere verificata e adeguata periodicamente.

[2] In particolare devono essere soddisfatti i seguenti requisiti:

a. le piattaforme di sviluppo, di controllo e di produzione sono separate tra loro;

---

2 La norma può essere consultata e richiesta presso l'Associazione svizzera di normazione (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

3 La norma può essere consultata e richiesta presso l'Associazione svizzera di normazione (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

4 La norma può essere consultata e richiesta presso l'Associazione svizzera di normazione (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

b. la rete è segmentata conformemente ai risultati di una valutazione dei rischi. I server utilizzati per l'esercizio della piattaforma di trasmissione sono distribuiti tra i segmenti della rete conformemente alla protezione di cui devono beneficiare;
c. i messaggi elettronici sono trasmessi e salvati unicamente in forma codificata. Non è necessaria una codificazione da un capo all'altro (end-to-end);
d. le password non sono registrate o protocollate in logfile senza essere codificate;
e. i metodi e i sistemi di crittografia impiegati sono conformi allo stato della tecnica e si fondano sui rischi attuali. Sono impiegati metodi e sistemi standardizzati quali quelli menzionati nella pubblicazione ufficiale dell'agenzia federale tedesca per le reti di elettricità, gas telecomunicazioni, posta e ferrovie[5] «Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)», comprendente una panoramica degli algoritmi adeguati, o in standard paragonabili. Qualsiasi impiego di una norma divergente deve essere motivata oggettivamente e la sua l'idoneità e l'efficacia devono essere verificate. La resistenza dei metodi e sistemi proprietari utilizzati agli attacchi crittoanalitici noti è comprovata;
f. la piattaforma di trasmissione è concepita in modo che sia possibile, con un onere ragionevole, sostituire le procedure e i sistemi crittografici utilizzati e la lunghezza delle loro chiavi;
g. nel quadro della trasmissione, per evitare attacchi del tipo «offline password guessing» è inammissibile una codificazione dei messaggi basata unicamente su chiavi dedotte dalle password;
h. la solidità dei metodi e dei sistemi crittografici impiegati è descritta in modo completo e dettagliato nel quadro della creazione dell'architettura globale della sicurezza. Nel senso di un processo di ottimizzazione continuo, le procedure e i sistemi crittografici sono verificati periodicamente e se del caso adeguati.

4.3.2 Gestione dell'accesso

[1] Le misure di gestione dell'accesso adottate dalla piattaforma di trasmissione devono orientarsi allo stato della tecnica e ai rischi attuali, essere oggetto di una descrizione completa e dettagliata ed essere verificate periodicamente. Se del caso vanno adeguate.

[2] In particolare devono essere adempiuti i seguenti requisiti:

a. l'accesso ai messaggi elettronici in trasmissione avviene tramite procedure di autentificazione forti (p. es. certificati digitali o token personali). L'informazione di autentificazione non è trasmessa in testo chiaro per prevenire attacchi di intercettazione o riproduzione;
b. se l'autentificazione si basa su password, queste devono essere trasmesse tramite collegamenti cifrati (p. es. nel quadro di un collegamento Secure Sockets Layer [SSL] / Transport Layer Security [TLS]). Si può rinunciare a una limitazione temporale della validità delle password, la cui forza deve soddisfare i requisiti attualmente usuali;
c. vanno adottate misure adeguate per prevenire il cracking della password e per impedire l'utilizzo di password banali. Gli utenti vanno invitati a utilizzare password forti (p. es. mediante un misuratore della forza delle password [password meter]): una password deve comprendere al minimo 8 caratteri di cui almeno 3 degli elementi seguenti: lettere maiuscole, lettere minuscole, cifre, caratteri speciali). Agli utenti deve essere comunicato che la password è personale e non può essere trasmessa.

[5] Gli algoritmi e parametri adeguati sono elencati in tedesco all'indirizzo: www.bundesnetzagentur.de > Die Bundesnetzagentur > Qualifizierte elektronische Signatur > Aufgaben der Bundesnetzagentur / Veröffentlichungen > Festlegung geeigneter Algorithmen.

4.3.3 Acquisizione, sviluppo e manutenzione dei componenti di piattaforma

a. I server raggiungibili tramite Internet devono essere resi sicuri a seconda delle necessità. Devono essere considerate le migliori prassi, per esempio i Security Configuration Benchmark messi a disposizione dal Center for Internet Security[6].
b. I componenti della piattaforma sono in grado di respingere gli attacchi noti con applicazioni Web, per esempio quelle documentate nel quadro del Open Web Application Security Project[7].

4.4 Eccezioni per autorità

Le piattaforme di trasmissione esclusivamente controllate da un'autorità possono salvare i messaggi elettronici in forma non cifrata e trasmetterli a sistemi interni. Al fine di garantire la sicurezza delle informazioni, l'autorità deve adottare misure amministrative, dirigenziali o tecniche adeguate ed efficaci per ridurre il rischio risultante da questa lacuna tecnica a un rischio residuo coerente con i criteri di accettazione dei rischi dell'autorità. Per determinare tali misure l'autorità si deve fondare su una valutazione del rischio conformemente alla SN EN ISO/IEC 27001, 2013.

6 www.cisecurity.org
7 www.owasp.org

5 Requisiti delle ricevute

5.1 Contenuto delle ricevute

Una ricevuta deve contenere:

a. informazioni sulla ricevuta
   1. denominazione della piattaforma di trasmissione che ha rilasciato la ricevuta,
   2. indicazione sul tipo di ricevuta: di consegna, di ritiro, di scadenza o di rifiuto;

b. informazioni sul messaggio elettronico:
   1. informazioni sul mittente del messaggio (nome, indirizzo e-mail),
   2. informazioni sul destinatario del messaggio (nome, indirizzo e-mail),
   3. campo oggetto (se compilato),
   4. marcatempo;

c. componenti o informazioni sui singoli componenti del messaggio (se non è cifrato end-to-end)
   1. denominazioni dei componenti (se esistenti),
   2. tipo e formato del componente,
   3. grandezza del componente in bytes,
   4. valore/i hash del componente, se possibile creato/i con due diverse funzioni hash crittografiche;

d. indicazione temporale del rilascio della ricevuta;

e. una firma elettronica avanzata secondo la legge federale del 19 dicembre 2003 sulla firma elettronica (FiEle; RS 943.03).

5.2 Indicazioni temporali

a. La firma elettronica della ricevuta si fonda su un certificato di un fornitore di servizi riconosciuto secondo la FiEle ed è collegata con un corrispondente marcatempo.

b. L'indicazione temporale che figura sulla ricevuta proviene dal marcatempo della piattaforma di trasmissione del fornitore di servizi e corrisponde al momento della consegna o del ritiro.

5.3 Cronologia delle fasi della comunicazione

Dal punto di vista cronologico, le fasi della comunicazione sono definite come segue:

a. domanda a un tribunale o a un'autorità:
   1. *momento della consegna:* momento in cui la piattaforma di trasmissione utilizzata dal mittente conferma che la domanda è stata caricata;
   2. *momento del ritiro:* momento in cui la piattaforma di trasmissione utilizzata dal tribunale o dall'autorità conferma che la domanda è stata ritirata;

b. convocazioni, decisioni o altre comunicazioni (comunicazioni) da parte di un tribunale o un'autorità:
   1. *momento della consegna:* momento in cui la piattaforma di trasmissione utilizzata dal tribunale o dall'autorità conferma che la comunicazione è stata caricata;
   2. *momento della distribuzione:* momento in cui la piattaforma di trasmissione utilizzata dal destinatario ha preparato il messaggio e avviato il processo d'invio o lo ha messo a disposizione del destinatario sulla piattaforma per essere scaricato;
   3. *momento del ritiro:*momento in cui la piattaforma di trasmissione utilizzata dal destinatario conferma che la comunicazione è stata ritirata se ciò avviene entro il termine legale di ritiro;
   4. *momento della decadenza:* momento in cui scade il termine legale di ritiro senza che la comunicazione sia stata ritirata.;
   5. *momento del rifiuto:* momento in cui la comunicazione è rifiutata entro il termine legale.

5.4 Ricevute da rilasciare

[1] Le piattaforme di trasmissione rilasciano le seguenti ricevute:

a. domanda a un tribunale o a un'autorità:
   1. ricevuta con l'indicazione del momento della consegna (ricevuta di consegna);
   2. ricevuta con l'indicazione del momento del ritiro (ricevuta di ritiro).
b. comunicazioni da parte di un tribunale o un'autorità:
   1. ricevuta con l'indicazione del momento della consegna(ricevuta di consegna);
   2. ricevuta con l'indicazione del momento
      - del ritiro, se la comunicazione è ritirata dal destinatario entro il termine legale (ricevuta di ritiro);
      - della decadenza, se la comunicazione non è ritirata dal destinatario entro il termine legale (ricevuta di decadenza); o
      - del rifiuto, se la comunicazione è rifiutata dal destinatario entro il termine legale (ricevuta di rifiuto).

[2] Se una piattaforma deve essere riconosciuta solo per la trasmissione di domande alle autorità (piattaforma di consegna), in deroga al capoverso 1 lettera a occorre unicamente rilasciare la ricevuta di consegna.

5.5 Allestimento e invio delle ricevute

a. La ricevuta è allestita dalla piattaforma di trasmissione come documento in formato PDF firmato elettronicamente.
b. Il tempo marcato nella firma della ricevuta non diverge di più di un minuto dal tempo indicato nella ricevuta. In altri termini, quest'ultima è preparata entro un minuto dalla firma. Questi termini costituiscono la regola. Le eventuali divergenze devono essere verbalizzate. Divergenze superiori a cinque minuti devono essere segnalate per scritto all'autorità di autorizzazione il giorno lavorativo successivo.
c. Nel quadro di una domanda a un tribunale o a un'autorità, il mittente e il tribunale o l'autorità ricevono le medesime ricevute menzionate al numero 5.4 capoverso 1 lettera a.

Il mittente può indicare alla piattaforma che rinuncia all'invio di una ricevuta di ritiro, nel caso di domande, o di una ricevuta di consegna, nel caso di comunicazioni.

d. Nel quadro di comunicazioni da parte di un tribunale o un'autorità, il tribunale o l'autorità e il destinatario ricevono le medesime ricevute menzionate al numero 5.4 capoverso 1 lettera b.
   Il tribunale o l'autorità possono indicare alla piattaforma che rinunciano all'invio di una ricevuta di ritiro, nel caso di domande, o all'invio di una ricevuta di consegna, nel caso di comunicazioni. Se la piattaforma dispone della funzione «Autoaccept», la ricezione può essere confermata senza un'indicazione temporale.
e. Se un messaggio elettronico è destinato contemporaneamente a più destinatari, è possibile riunire i differenti momenti di consegna in un'unica ricevuta. Il momento indicato in quest'ultima corrisponde al momento della conclusione del processo di unione dei differenti momenti di consegna.
f. Le ricevute sono messe a disposizione dei destinatari tramite la piattaforma di trasmissione da loro utilizzata.
g. Le ricevute possono essere inviate senza cifratura se non contengono dettagli sul contenuto della domanda o della comunicazione a parte il contenuto della ricevuta di cui al numero 5.1.
h. Su richiesta, le piattaforme possono inviare le ricevute a qualsiasi indirizzo e-mail indicato dai partecipanti alla trasmissione.
i. Il nome del file della ricevuta deve consentirne un'identificazione univoca e può avere il seguente formato:
   [YYMMDD]_[Message Identifier]_[piattaforma di trasmissione]_[tipo di ricevuta].

6 Requisiti per l'IT Service Management

6.1 Requisiti di base

[1] Per garantire un esercizio affidabile della piattaforma di trasmissione deve essere provato che i seguenti processi sono documentati, introdotti, gestiti, costantemente sorvegliati, periodicamente controllati, mantenuti e migliorati.

a. Processi di fornitura di un servizio:
   1. gestione dei livelli di servizio,
   2. rendiconto sul servizio,
   3. gestione della continuità del servizio e della disponibilità,
   4. preventivazione e fatturazione dei servizi IT,
   5. gestione delle capacità,
   6. gestione della sicurezza delle informazioni;

b. processi relativi alla gestione delle relazioni:
   1. cura delle relazioni tra fornitore di prestazioni e clienti,
   2. gestione dei fornitori;

c. processi di risoluzione:
   1. gestione degli eventi e delle domande di supporto,
   2. gestione dei problemi;

d. processi di conduzione:
   1. gestione delle configurazioni,
   2. gestione dei cambiamenti,
   3. gestione della liberazione e della preparazione.

[2] I processi devono orientarsi alle norme internazionali SN EN ISO/IEC 20000-1, 2011 (Information technology – Service management – Part 1: Service management system requirements[8]) e ISO/IEC 20000-2, 2012 (Information technology – Service management – Part 2: Guidance on the application of service management systems[9]) o a norme comparabili. Una relativa certificazione è auspicabile ma non necessaria.

[3] Inoltre deve essere introdotto, gestito, costantemente sorvegliato, periodicamente controllato, mantenuto e migliorato un Service Desk professionale.

6.2 Disponibilità

[1] In linea di principio, una piattaforma di trasmissione deve essere disponibile tutti i giorni 24 ore su 24. Eventuali interruzioni per lavori di manutenzione devono essere pianificate tra le 00:15 e le 07:00 (ora Svizzera) o durante i fine settimana. Devono essere annunciate sulla piattaforma almeno 72 ore prima.

---

8 La norma può essere consultata e richiesta presso l'Associazione svizzera di normazione (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

9 La norma può essere consultata e richiesta presso l'Associazione svizzera di normazione (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

[2] La disponibilità della piattaforma deve essere indicata su un protocollo che va pubblicato sulla stessa.

6.3 Sincronizzazione dell'orologio

L'orologio della piattaforma deve essere sincronizzato con un server di riferimento di modo che tra i due non ci sia mai una differenza superiore a 5 secondi. Il meccanismo di sincronizzazione e le differenze di tempo rilevate devono essere verbalizzati.

6.4 Dimensioni dei messaggi elettronici

La piattaforma deve poter elaborare messaggi elettronici di 15 MB e inviare/trasmettere messaggi di 25 MB.

6.5 Informazioni per utenti

[1] Il fornitore di prestazioni deve pubblicare sulla piattaforma, in una forma comprensibile per i profani, le caratteristiche principali:

a. dell'architettura;
b. dei controlli d'accesso;
c. delle procedure e dei sistemi crittografici.

[2] Occorre inoltre segnalare che una cifratura end-to-end dei messaggi elettronici non è necessaria e al contempo pubblicare la seguente indicazione:
Un messaggio non cifrato può essere presente sulla piattaforma di trasmissione in forma non cifrata e dunque essere visionato dal fornitore di prestazioni o da un terzo incaricato, nonostante ciò sia vietato. Gli utenti che non intendono rischiare che i loro messaggi siano visionati devono rinunciare a utilizzare la piattaforma di trasmissione o cifrare ulteriormente i messaggi (p. es. con una chiave di creazione della firma pubblica del destinatario).

[3] Gli utenti della piattaforma devono essere informati in merito ai loro obblighi di diligenza e di cooperazione, nonché sul fatto che i dati che li concernono sono visibili nell'elenco principale dei partecipanti (cfr. n. 7). Occorre inoltre attirare la loro attenzione sulla necessità di utilizzare password forti e sul fatto che quanto figura nel campo «Oggetto» del messaggio e i nomi dei file degli eventuali allegati non sono trasmessi in forma cifrata.

7 Requisiti dell'elenco principale dei partecipanti

[1] Per la trasmissione di messaggi elettronici tra le piattaforme, l'UFG gestisce un elenco principale dei partecipanti, non pubblico, a cui si può avere accesso unicamente tramite piattaforme riconosciute. L'utilizzo dei dati ivi contenuti per scopi di pubblicità o marketing non è ammesso.

[2] L'elenco principale dei partecipanti deve mettere a disposizione delle piattaforme gli elenchi dei partecipanti come sottocategorie separate con diritto di scrittura. Queste sottocategorie si fondano su una classe di oggetti Lightweight Directory Access Protocol (LDAP) con i seguenti attributi (sono possibili altri attributi, p. es. le coordinate di un service desk, eventuali preferenze di visualizzazione e di ricerca, limitazioni alle dimensioni di messaggi e commenti).

Nome dell'attributo	Significato	Esempi
Ou	Nome canonico della piattaforma.	ekomm, Incamail, Cantone di Berna, PrivaSphere
platformUri	URI, alla quale è raggiungibile la piattaforma.	https://www.bla.ch:8080/
smtpUri	Indirizzo del MTA della piattaforma preparato per l'interoperabilità.	smtps://smtp.bla.ch:25001/
smimeSignCertificate smimeEncryptionCertificate	Certificati X.509 per le chiavi pubbliche utilizzate dalla piattaforma per S/MIME per firmare o cifrare e decifrare (possono anche essere identici). Formato: PKCS#7 SignedData	
smtpCertificate	Certificato X.509 per la chiave pubblica utilizzata dal MTA della piattaforma per la trasmissione sicura di messaggi ad altre piattaforme. Formato: PKCS#7 Signed-Data.	

[3] Le iscrizioni nelle sottocategorie dell'elenco si fondano sulla classe di oggetti inet-OrgPerson secondo RFC 2798. I seguenti due attributi sono necessari:

a. Mail (mail);
b. Distinguished Name (dn).

[4] Ogni partecipante deve essere univocamente identificabile tramite l'attributo Mail. Tipicamente, il Distinguished Name è creato utilizzando l'attributo Mail.

[5] Ogni piattaforma deve mettere a disposizione nell'elenco principale i dati dei suoi partecipanti e aggiornarli almeno una volta al giorno.

[6] I gestori delle piattaforme devono identificare i partecipanti. A tal fine possono utilizzare in particolare le seguenti procedure:

a. identificazione personale secondo i requisiti di cui all'articolo 5 dell'ordinanza del 3 dicembre 2004 sulla firma elettronica (OFiEle; RS 943.032);
b. identificazione mediante SuisseID;
c. validazione dell'indirizzo di domicilio mediante una lettera;
d. relazione contrattuale scritta stipulata tra il partecipante e il gestore della piattaforma;
e. registrazione di gruppo (conferma delle identità da parte di federazioni cantonali degli avvocati o avvocati registrati e identificati).

[7] La comunicazione nei due sensi tra l'elenco principale dei partecipanti e gli elenchi delle piattaforme avviene tramite una procedura di autentificazione forte, idealmente basata su un protocollo LDAPS (LDAP over SSL) e su certificati di un servizio di certificazione riconosciuto secondo FiEle.

[8] Se un'autorità mette a disposizione in Internet un modulo per le domande a essa destinate, nell'elenco principale dei partecipanti deve figurare anche il relativo URL.

8 Requisiti della comunicazione tra piattaforme

[1] Se il mittente e il destinatario di un messaggio elettronico sono registrati sulla medesima piattaforma, il messaggio è trasmesso senza abbandonare tale piattaforma. In caso contrario, il messaggio deve essere trasmesso tra le piattaforme. Di regola un messaggio è trasmesso tra due piattaforme, ma non è escluso l'impiego di un numero maggiore di piattaforme.

[2] Qui di seguito, A designa il mittente di un messaggio, Z_A la piattaforma su cui è registrato A o tramite la quale è inviato il messaggio, B il destinatario e Z_B la piattaforma su cui è registrato B ($Z_A \neq Z_B$). Di norma, Z_A e Z_B sono connesse tra loro e possono scambiarsi messaggi. Se non sono connesse, per trasmettere il messaggio occorre coinvolgere anche altre piattaforme.

8.1 Requisiti di base

[1] La comunicazione tra le piattaforme deve essere protetta mediante crittografia con una procedura a due livelli.

1. A livello di trasporto, i dati sono cifrati conformemente alla RFC 3207 (Secure Simple Mail Transfer Protocol [SMTP] over TLS). A tal scopo ogni piattaforma di trasmissione deve gestire un SMTP Mail Transfer Agent (MTA) che supporta Secure SMTP over TLS. L'indirizzo di questo MTA deve essere pubblicato nell'elenco principale dei partecipanti assieme a un certificato X.509 smtpCertificate. Con l'ausilio dei certificati X.509 gli MTA si autentificano a vicenda.
2. A livello di utenza, i messaggi sono cifrati conformemente alla Secure Multipurpose Internet Mail Extensions (MIME) Standard (S/MIME): un messaggio elettronico è firmato dalla piattaforma mittente con una chiave di creazione della firma privata e cifrato con la chiave di cifratura pubblica della piattaforma destinataria. I corrispondenti certificati X.509 smimeSignCertificate e smimeEncryptionCertificate devono essere pubblicati nell'elenco principale dei partecipanti.

[2] Di conseguenza ogni piattaforma deve disporre di tre paia di chiavi: una per la cifratura dei dati a livello di trasporto e due per la firma e la cifratura dei messaggi a livello di utenza (nella tabella al punto 7 figurano i corrispondenti certificati: smtpCertificate, smimeSignCertificate e smimeEncryptionCertificate). Nell'ambito di un'implementazione concreta, un certificato può essere impiegato per diversi scopi.

[3] Qui di seguito, la cifratura dei dati a livello di trasporto non è più considerata. Essa comporta essenzialmente una configurazione dei MTA a supporto di STARTTLS (Secure SMTP over TLS). Per la cifratura dei messaggi nella fase dell'applicazione deve essere impiegato il protocollo di trasmissione descritto qui di seguito.

8.2 Protocollo di trasmissione

[1] Qui di seguito è abbozzato il caso della trasmissione di un messaggio tramite due piattaforme Z_A e Z_B. Z_B deve rilasciare una ricevuta di ritiro e verbalizzare il momento della trasmissione, mentre Z_A deve rilasciare una ricevuta di consegna.

a. La trasmissione del messaggio tra due piattaforme Z_A e Z_B si svolge come segue.
   1. Z_A riceve il messaggio elettronico da trasmettere, invia una ricevuta di consegna e lo inserisce in un messaggio conforme a S/MIME con le seguenti intestazioni SMTP:
      - To: indirizzo e-mail di B;
      - From: indirizzo e-mail di A;
      - Message-ID: un identificatore (Identifier) univoco per il messaggio stabilito da Z_A e valido per tutte le piattaforme;
      - X-ZP-MsgType: tipo di messaggio, nel caso della trasmissione di un messaggio elettronico va utilizzato «message»;
      - momento della consegna o del ritiro o della decadenza o del rifiuto (cfr. n. 5.3; indicando data, ora e minuti) in millisecondi dal 1.1.1970 (X-ZP-IntakeTimeStampMillis, X-ZP-ReceiveTimeStampMillis)[10], affinché i tempi possano essere indicati con sistematicità anche per messaggi trasmessi da una piattaforma all'altra[11];
      - Sender Platformname (X-ZP-FromPlatform) comprendente l'iscrizione «OU» univoca della piattaforma nell'elenco principale dei partecipanti.

      Sono possibili intestazioni supplementari (p. es. per indicare il tempo locale di Z_A o se si tratta di una domanda o di una comunicazione[12]). Il messaggio elettronico effettivamente da trasmettere costituisce il corpo del messaggio conforme a S/MIME.
   2. Z_A firma il messaggio conforme a S/MIME con la sua chiave di creazione della firma privata e cifra il risultato con la chiave di cifratura pubblica di Z_B.
   3. Il messaggio firmato e cifrato è trasmesso dal MTA di Z_A al MTA di Z_B, utilizzando la cifratura dei dati a livello di trasporto (STARTTLS o Secure SMTP over TLS). Eventuali firme che servono a garantire la sicurezza a livello di trasporto non devono essere considerate. In caso contrario – ossia se il messaggio non può essere consegnato al destinatario – A deve esserne informato il più presto possibile.
   4. Z_B decifra il messaggio ricevuto, verifica e rimuove la firma, verbalizza il momento della consegna e consegna il messaggio a Z_A. Al contempo, il messaggio è depositato nella casella postale di B e può essere consultato o, in caso di accordo esplicito, direttamente preso in consegna da B.
   5. La piattaforma destinataria Z_B garantisce che i messaggi firmati dal mittente possano essere letti quando sono ricevuti tramite le interfacce Internet.
   6. Z_B accetta il messaggio indipendentemente dallo statuto del mittente nell'elenco principale dei partecipanti.

b. Dopo essere stato trasmesso a Z_B, il messaggio è di competenza di quest'ultima piattaforma, alla quale spetta informare Z_A in merito alle eventuali azioni di cui è oggetto. A tal

---

10 Per facilitare l'handling, i medesimi tempi dovrebbero figurare in un ulteriore X-Header in una forma leggibile da un essere umano.

11 I momenti della consegna o della trasmissione della piattaforma locale possono essere rappresentati in particolare sul WEB-GUI della piattaforma (p. es. con pop-up «mouseover» o «more info»). Per il profano sono però a prima vista visibili soltanto i tempi coordinati tra le piattaforme.

12 Se p. es. il mittente e il destinatario sono autorità non è automaticamente chiaro se si tratta di una domanda o una sentenza o una decisione. In questo caso, per garantire un corretto funzionamento di «receipt-auto-delivered» è utile l'intestazione opzionale «X ZP TypeOfCommunication" con i valori «ENQUIRY» e «AUTHORITY_RESPONSE».

scopo Z_B può creare un messaggio conforme a S/MIME con le seguenti intestazioni SMTP e rinviarlo a Z_A.

1. To: indirizzo e-mail di A.
2. From: indirizzo e-mail di B.
3. Message-ID: un identificatore (Identifier) univoco per il messaggio stabilito da Z_B e valido per tutte le piattaforme.
4. In-Reply-To: il valore dato da Z_A nel campo Message-ID.
5. X-ZP-MsgType: uno dei seguenti tipi di messaggio:
   - receipt-deposited: il messaggio è depositato nella casella postale di B;
   - receipt-delivered: il messaggio è stato ritirato da B;
   - receipt-auto-delivered: il messaggio è stato automaticamente inoltrato a B (p. es. un'autorità. Z_B può rinunciare a rilasciare una ricevuta di ritiro;
   - receipt-timed-out: il termine di consegna per il messaggio è scaduto inutilizzato;
   - receipt-refused: B ha rifiutato di prendere in consegna il messaggio;
   - receipt-invalid-signature: la firma del messaggio non è valida;
   - receipt-error: segnalazione di errore generico indipendente dalla firma;
   - confidential: questo tipo di messaggio è per esempio utilizzato per la ricevuta di consegna, se questa è trasmessa tramite l'altra piattaforma.
     Al fine di garantire la maggiore solidità possibile, queste comunicazioni interoperabili devono essere obbligatoriamente protette solo a livello di trasporto senza l'impiego del smimeEncryptionCertificate.

c. Se X-ZP-MsgType ha il valore «receipt-delivered», il corpo del messaggio deve contenere la corrispondente ricevuta di consegna ed eventualmente informazioni supplementari (p. es. sottoforma di intestazioni SMTP supplementari). Se X-ZP-MsgType ha il valore «receipt-error», il corpo del messaggio può contenere ulteriori informazioni sull'errore occorso. Se è impiegata l'intestazione X-Zp-ERROR-To-User, questa è mostrata all'utente interessato. In questo come in tutti gli altri casi il corpo del messaggio può pure essere vuoto.

d. In ogni caso, Z_B firma il messaggio con la sua chiave di creazione della firma privata e cifra il risultato con la chiave di cifratura pubblica di Z_A. Il messaggio firmato e cifrato è trasmesso dal MTA di Z_B al MTA di Z_A (di nuovo tramite un canale protetto crittograficamente a livello di trasporto con l'ausilio di Secure SMTP over TLS). Infine, Z_A decifra il messaggio, controlla e rimuove la firma e comunica le azioni ad A in forma adeguata o gli trasmette la ricevuta.

[2] Supporto per l'invio ad autorità: se dopo due giorni (lavorativi) la piattaforma mittente constata che un'autorità destinataria non ha ancora ritirato un messaggio ad essa destinato, può aprire un ticket di allerta presso la piattaforma destinataria. Quest'ultima garantisce che sia aperto, entro il termine restante, un ticket presso l'organizzazione di supporto dell'autorità con cui ha stipulato il contratto. Prima della scadenza del termine informa la piattaforma mittente sullo stato della questione.

8.3 Utilizzo delle funzioni di trasmissione e degli elenchi dei partecipanti

[1] Le piattaforme si mettono gratuitamente a disposizione a vicenda le funzioni di trasmissione conformemente al suddetto protocollo e le informazioni per l'elenco principale dei partecipanti.

[2] Per gli utenti finali sono ammesse ricerche con caratteri jolly nell'elenco principale.